Due Date: October 1, 2007

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**
**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

| | | |
|---|---|---|
| In re Application of: | ) | |
| Inventor: Ronald P. Cocchi et al. | ) | Examiner: Syed Zia |
| Serial #: 10/085,920 | ) | Group Art Unit: 2131 |
| Filed: February 28, 2002 | ) | Appeal No.: _____ |
| Title: DEDICATED NONVOLATILE MEMORY | ) | |

**BRIEF OF APPELLANTS**

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In accordance with 37 CFR §41.37, Appellants hereby submit the Appellants' Brief on Appeal from the final rejection in the above-identified application, as set forth in the Office Action dated June 28, 2007.

Please charge the amount of $510.00 to cover the required fee for filing this Appeal Brief as set forth under 37 CFR §41.37(a)(2) and 37 CFR §41.20(b)(2) to Deposit Account No. 50-0383 of The DIRECTV Group, Inc., the assignee of the present application. Also, please charge any additional fees or credit any overpayments to Deposit Account No. 50-0383.

## I. REAL PARTY IN INTEREST

The real party in interest is The DIRECTV Group, Inc., the assignee of the present application.

## II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences for the above-referenced patent application.

## III. STATUS OF CLAIMS

Claims 1-28 are pending in the application.

Claims 1-7 were rejected under 35 U.S.C. §103(a) as being obvious in view of Kocher and Cohen et al., U.S. Patent 5,282,249 (Cohen).

Claims 8-28 were rejected under 35 U.S.C. §102(e) as being anticipated by Kocher, U.S. Patent 6,289,455 (Kocher).

All of the above rejections are being appealed.

## IV. STATUS OF AMENDMENTS

No amendments to the claims have been made subsequent to the final Office Action.

## V. SUMMARY OF CLAIMED SUBJECT MATTER

The claims are summarized in the following table:

| **CLAIM LIMITATION** | **SUPPORT IN SPECIFICATION** |
|---|---|
| 1. A system for controlling access to digital services comprising: | Page 1, lines 19-21. |
| (a) a control center configured to coordinate and provide digital services; | Page 5, lines 5-12;<br>Item 102 of Fig. 1. |
| (b) an uplink center configured to receive the digital services from the control center and transmit the digital services to a satellite; | Page 5, lines 5-19;<br>Item 104 of Fig. 1. |
| (c) the satellite configured to: | Page 5, lines 13-19;<br>Item 108 of Fig. 1. |
| (i) receive the digital services from the uplink center; | Page 5, lines 13-19;<br>Item 108 of Fig. 1. |

| | |
|---|---|
| (ii) process the digital services; and | Page 5, lines 13-19;<br>Item 108 of Fig. 1. |
| (iii) transmit the digital services to a subscriber receiver station; | Page 5, lines 13-19;<br>Item 108 of Fig. 1. |
| (d) the subscriber receiver station configured to: | Page 5, lines 13-25;<br>Item 110 of Fig. 1. |
| (i) receive the digital services from the satellite; | Page 5, lines 13-25;<br>Item 110 of Fig. 1. |
| (ii) control access to the digital services through an integrated receiver/decoder (IRD); | Page 5, lines 13-25;<br>Item 110 of Fig. 1. |
| (e) a conditional access module (CAM) communicatively coupled to the IRD, wherein the CAM comprises: | Page 5, lines 20-25;<br>Page 15, lines 9-16;<br>Item 126 of FIG. 1; Item 512 of FIG. 5. |
| (i) a protected nonvolatile memory component, wherein: | Page 15, lines 1-8;<br>Item 614 of FIG. 6. |
| (1) the protected nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services; | Page 17, lines 12-21;<br>Item 614 of FIG. 6;<br>Item 700 of FIG. 7. |
| (2) programming control and a programming charge pump are shared by both the protected nonvolatile memory component and a microprocessor's non-protected nonvolatile memory component; and | Page 16, lines 15-22;<br>FIG. 6 |

| | |
|---|---|
| (3) the microprocessor's non-protected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same; and | Page 16, lines 8-14;<br>Items 606 and 612 of FIG. 6 |
| (ii) a fixed state custom logic block configured to control access to the nonvolatile memory component, wherein data and address lines of the protected nonvolatile memory component are routed only to the fixed state custom logic block. | Page 15, lines 1-8;<br>Page 16, lines 15-22;<br>Items 614 of FIG. 6. |
| | |
| 8. A method for limiting unauthorized access to digital services comprising: | Page 1, lines 19-21. |
| (a) configuring a protected nonvolatile memory component, wherein: | Page 5, lines 20-25;<br>Page 15, lines 9-16;<br>Item 126 of FIG. 1; Item 512 of FIG. 5. |
| (i) the protected nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services; | Page 17, lines 12-21;<br>Item 614 of FIG. 6;<br>Item 700 of FIG. 7. |

| | |
|---|---|
| (ii) programming control and a programming charge pump are shared by both the protected nonvolatile memory component and a microprocessor's non-protected nonvolatile memory component; and | Page 16, lines 15-22;<br>FIG. 6 |
| (iii) the microprocessor's non-protected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same; | Page 16, lines 8-14;<br>Items 606 and 612 of FIG. 6 |
| (b) controlling access to the nonvolatile memory component through a fixed state custom logic block, and wherein data and address lines of the protected nonvolatile memory component are routed only to the fixed state custom logic block. | Page 15, lines 1-8;<br>Page 16, lines 15-22;<br>Items 614 of FIG. 6. |
| | |
| 15. A conditional access module (CAM), comprising: | Page 1, lines 19-21. |
| (a) a protected nonvolatile memory component, wherein: | Page 5, lines 20-25;<br>Page 15, lines 9-16;<br>Item 126 of FIG. 1; Item 512 of FIG. 5. |
| (i) the protected nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing digital services; | Page 17, lines 12-21;<br>Item 614 of FIG. 6;<br>Item 700 of FIG. 7. |

| | |
|---|---|
| (ii) programming control and a programming charge pump are shared by both the protected nonvolatile memory component and a microprocessor's non-protected nonvolatile memory component; and | Page 16, lines 15-22;<br>FIG. 6 |
| (iii) the microprocessor's non-protected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same; and | Page 16, lines 8-14;<br>Items 606 and 612 of FIG. 6 |
| (b) a fixed state custom logic block configured to control access to the nonvolatile memory component, and wherein data and address lines of the protected nonvolatile memory component are routed only to the fixed state custom logic block. | Page 15, lines 1-8;<br>Page 16, lines 15-22;<br>Items 614 of FIG. 6. |
| | |
| 22. An article of manufacture for preventing unauthorized access to digital services comprising: | Page 1, lines 19-21;<br>Page 3, lines 21-26. |

| | |
|---|---|
| (a) means for configuring a protected nonvolatile memory component, wherein: | This claim limitation is a mean plus function and the structure materials or acts described in the specification corresponding to this limitation can be found at:<br>Page 5, lines 20-25;<br>Page 15, lines 9-16;<br>Item 126 of FIG. 1; Item 512 of FIG. 5. |
| (i) the protected nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services; | Page 17, lines 12-21;<br>Item 614 of FIG. 6;<br>Item 700 of FIG. 7. |

| | |
|---|---|
| (ii) programming control and a programming charge pump are shared by both the protected nonvolatile memory component and a microprocessor's non-protected nonvolatile memory component; and | Page 16, lines 15-22;<br>FIG. 6 |
| (iii) the microprocessor's non-protected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same; and | Page 16, lines 8-14;<br>Items 606 and 612 of FIG. 6 |
| (b) means for controlling access to the nonvolatile memory component through a fixed state custom logic block, and wherein data and address lines of the protected nonvolatile memory component are routed only to the fixed state custom logic block. | This claim limitation is a mean plus function and the structure materials or acts described in the specification corresponding to this limitation can be found at:<br>Page 15, lines 1-8;<br>Page 16, lines 15-22;<br>Items 614 of FIG. 6. |

Thus, independent claims 1, 8, 15, and 22 are generally directed to controlling access to digital services. More specifically, the claims provide for a control center providing digital services to an uplink center that transmits the services to a satellite that sends it to a subscriber receiver station. A conditional access module (CAM) in the subscriber receiver station has specific functionality. Namely, a protected nonvolatile memory component contains state information that provides functionality and enforces security policies for accessing the digital services.

In addition, Appellants note that the independent claims provide further limitations. Namely, the claims provide for two nonvolatile memory components. One nonvolatile memory component is protected. The other nonvolatile memory component is unprotected and is referred

to as a microprocessor's non-protected nonvolatile memory component. The claims provide specific limitations and details regarding both the protected and unprotected nonvolatile memory components. In one limitation, the data and address lines of the protected component are only routed to the fixed state custom logic block.

In addition, the claims provide that the microprocessor's non-protected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same. As set forth in paragraph [0067] of the application as filed, they can be shared since they are controlled and programmed by separate entities. The use of the same physical and logical address range helps obscure use of the memory (e.g., containing a hidden number) by potential attackers making it more difficult to determine the memory map and usage of code segments within the CAM.

## VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1-7 are unpatentable under 35 U.S.C. §103(a) as being obvious in view of Kocher and Cohen et al., U.S. Patent 5,282,249 (Cohen).

Whether claims 8-28 are unpatentable under 35 U.S.C. §102(e) as being anticipated by Kocher, U.S. Patent 6,289,455 (Kocher).

Whether claims 1, 8, 15, and 22 are patentable under the judicially created doctrine of obviousness type double patenting over claims 1, 10, 19, and 28 of application serial number 10/085,346.

## VII. ARGUMENT

### A. Whether claims 1-7 are unpatentable under 35 U.S.C. §103(a) as being obvious in view of Kocher and Cohen et al., U.S. Patent 5,282,249 (Cohen).

#### 1. Claim 1

Appellants traverse the rejection of claim 1 for at least one or more of the following reasons:

(i) Neither Kocher nor Cohen teach, disclose or suggest that a microprocessor's non-protected nonvolatile memory component and a protected nonvolatile memory component use physical and logical address ranges that are the same;

(ii) Neither Kocher nor Cohen teach, disclose or suggest two different nonvolatile memory components that share programming control and a programming charge pump; and

(iii) Neither Kocher nor Cohen teach, disclose or suggest programming control and a programming charge pump that are shared by both the protected nonvolatile memory component and a microprocessor's non-protected nonvolatile memory component.

As stated above, Independent claims 1, 8, 15, and 22 are generally directed to controlling access to digital services. More specifically, the claims provide for a control center providing digital services to an uplink center that transmits the services to a satellite which sends it to a subscriber receiver station. A conditional access module (CAM) in the subscriber receiver station has specific functionality. Namely, a protected nonvolatile memory component contains state information that provides functionality and enforces security policies for accessing the digital services.

In addition, Appellants note that the claims provide further limitations. Namely, the claims provide for two nonvolatile memory components. One nonvolatile memory component is protected. The other nonvolatile memory component is unprotected and is referred to as a microprocessor's non-protected nonvolatile memory component. The claims provide specific limitations and details regarding both the protected and unprotected nonvolatile memory components. In one limitation, the data and address lines of the protected component are only routed to the fixed state custom logic block. Such a limitation provides a unique capability that is not disclosed in Kocher.

In addition, the amended claims provide that the microprocessor's non-protected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same. As set forth in paragraph [0067] of the application as filed, they can be shared since they are controlled and programmed by separate entities. The use of the same physical and logical address range helps obscure use of the memory (e.g., containing a hidden number) by potential attackers making it more difficult to determine the memory map and usage of code segments within the CAM.

The cited references fail to teach these various elements of the claims.

The Office Action relies on Kocher to teach the protected nonvolatile memory component. However, nowhere in Kocher is there any discussion where logical and physical address ranges of a

protected component and an unprotected component are the same. In fact an electronic search of Kocher for the term "logical" provided no results. Accordingly, without even mentioning a logical address range, Kocher cannot possibly teach that the same logical address range is used by two different and distinct nonvolatile memories. Further, advantages of such an embodiment are neither taught, described, or remotely alluded to in Kocher.

In addition to the above, Appellants note that the other cited references (i.e., Cohen) fail to cure the deficiencies of Kocher.

With respect to the programming charge pump, Appellants note that neither Cohen nor Kocher teach, describe, suggest, or allude to a programming charge pump whatsoever. The prior final office Action states:

In the disclosure Appellant merely mentioned charge pump (only at paragraph 0068) and does not describe how this charge pump is different than any other charge pump already known in the art. Charge pumps use some form of switching device(s) to control the connection of voltages to the capacitor, such as memory, in a I/O environment, such as hardware architecture of Kochner (Fig.2).

Wikipedia defines a charge pump as:

> A **charge pump** is an electronic circuit that uses capacitors as energy storage elements to create either a higher or lower voltage power source.

Appellants are not contending that the charge pump is different than another charge pump already known in the art. What Appellants are asserting is that the prior art fails to teach the sharing of a programming charge pump and programming control on both a non-protected nonvolatile memory component and a protected nonvolatile memory component. In addition, Appellants previously amended the claims to provide that data and address lines of the protected nonvolatile memory component are routed only to the fixed state custom logic block. The prior art fails to teach such an implementation. Paragraphs [0068]-[0069] of the originally filed specification describe the advantages of such shared control:

> **[0068]** Additionally, the two nonvolatile memory components 606 and 614 may share programming charge pumps and programming control. If the pumps and/or programming control are shared, care should be taken to ensure that data and address lines of the dedicated nonvolatile memory component 614 are routed only to the custom logic block 612. This saves chip area and reduces chip cost. Accordingly, the microprocessor 602 cannot provide control information that may lead to a

> subsequent attack on the dedicated memory component 614. Sharing the charge pumps may be preferred to ease timing and high voltage requirements of the entire chip within CAM 512.
> **[0069]** There are many advantages to dedicating a modifiable protected nonvolatile memory component 614 to a custom logic block 612. For example, the protected nonvolatile memory component 614 can withstand substantial external attacks without inappropriately modifying the contents of the dedicated memory components 614. Further, the identity of the device (i.e., the CAM 512) is protected for use in operations with the CAM 512, IRD 126, and headend. For example, the CAM 512 provides non-modifiable uniqueness (i.e., stored in protected memory 614) that can be used to prevent cloning of the CAM 512 to obtain unauthorized access. Additionally, the CAM 512 may provide an IRD 126 for non-modifiable pairing and blacklist, and may provide a headend that controls access rights and blacklist. A blacklist is utilized to prevent CAMs 512 with a particular identification to be used/cloned. With a blacklist, the headend may provide a list of blacklisted/unauthorized cards to an IRD 126. The IRD 126 then refuses to grant access rights if the CAM 512 being utilized is on the blacklist. Accordingly, uniquely identified CAMs 512 with a unique identification that is only accessible through a custom logic block 612 may be utilized to prevent unauthorized access and cloning. By preventing the system I/O module 608, system bus 610, microprocessor 602, or memory access control unit from directly accessing the protected nonvolatile memory component 614, traditionally successful security comprises are no longer possible.

Again, the novel features of the invention do not lie in the mere use of the charge pump. Instead, Appellants submit that the sharing of the programming control and programming charge pump across the two unique nonvolatile memory components are not even remotely contemplated by the cited prior art. Further, the routing of the data and address lines of the protected component while still sharing the same programming charge pump provides unique advantages to the system and design of the present invention. In this regard, the specification provide that such a design saves chip area and reduces chip cost while avoiding the ability for a microprocessor to provide control information that leads to a subsequent attack on the memory component. Such advantages are clearly absent from the prior art and any known method of use of charge pumps.

In addition, Appellants note that the prior final Office Action admits that Kocher fails to teach the use of a charge pump. In this regard, the Action provides that charge pumps and the combination or manner in which they are used is known in the art. Such an assertion is wholly without merit.

The prior final Office Action continues and asserts that a switching device is equivalent to a programming charge pump. As previously indicated, a programming charge pump is not equivalent to a switching device. Further, Appellants submit that the prior art fails to teach the sharing of a programming charge pump and programming control on both a non-protected nonvolatile memory component and a protected nonvolatile memory component. In addition, the claims provide that

data and address lines of the protected nonvolatile memory component are routed only to the fixed state custom logic block. The prior art fails to teach such an implementation. Paragraphs [0068]-[0069] of the originally filed specification describe the advantages of such shared control.

Again, the novel features of the invention do not lie in the mere use of the charge pump. Instead, Appellants submit that the sharing of the programming control and programming charge pump across the two unique nonvolatile memory components are not even remotely contemplated by the cited prior art. Further, the routing of the data and address lines of the protected component that use the same physical and logical address ranges while still sharing the same programming charge pump provides unique advantages to the system and design of the present invention. In this regard, the specification provide that such a design saves chip area and reduces chip cost while avoiding the ability for a microprocessor to provide control information that leads to a subsequent attack on the memory component. Such advantages are clearly absent from the prior art and any known method of use of charge pumps.

In addition, Appellants note that a prior Office Action admits that Kocher fails to teach the use of a charge pump. In this regard, the Action provides that charge pumps and the combination or manner in which they are used is known in the art. Such an assertion is wholly without merit as described above and as asserted in the prior responses.

In response to the above arguments, the Office Action mailed on June 28, 2007 merely addresses the arguments relating to the same physical and logical address ranges maintaining that the arguments above were not persuasive:

> This is not found persuasive. Cited prior art teaches a system and method that relates to cryptographic unit connected in between a microprocessor and memory for protecting the memory from microprocessor by cryptographically transforming data communicated in between microprocessor and memory. The cryptographic unit for transforming data from microprocessor uses memory contents and transformation result is utilized to decode digital content. Cryptographic right unit CRU includes an interface control processor (ICP), which is responsible for communication with playback device via 110 interface. In addition, CRU includes several types of memory connected to interface control processor via bus. In particular, fixed data and code are stored in ROM, temporary data (and possibly code) are stored in RAM, and additional code and/or data are stored in EEPROM which can be modified by processor. Also attached to bus is CryptoFirewall, a specialized cryptographic processing unit which regulates and cryptographically modifies data written to or read from protected memory (co1.9 line 29 to line 59 and (co1.27 line 25 to line 39).
>
> Kocher further teach or disclose of switching device(s) (such as programming charge pump) to control the connection of voltages to memory in a I/O environment, such as hardware architecture of Kochner (Fig.2, co1.21 line 34 to line 64).

> Thus the system of cited prior art provides a system and method for preventing unauthorized access to digital services.
>
> Therefore, the examiner asserts that cited prior art does teach or suggest the subject matter recited in independent Claims 1,8, 15,22, and in subsequent dependent Claims. Accordingly, rejections for claims 1-28 are respectfully maintained.

Appellants respectfully disagree with and traverse such assertions. Further, nothing in such an argument even remotely addresses the arguments set forth above. In this regard, the Examiner fails to address the limitations relating to the microprocessor's non-protected nonvolatile memory component and protected nonvolatile memory component using physical and logical address ranges that are the same. Thus, the Examiner merely disregards the previously presented arguments. Accordingly, Appellants reassert the arguments set forth above.

In view of the above, Appellants respectfully request reversal of the rejections.

2. Claim 2

This claim provides that the custom logic block has a fixed algorithm that cannot be altered by external means. In rejecting this claim, the Office Action relies on Kocher col. 23, lines 36 to 48. These lines provide:

> Under the architecture outlined in FIG. 2, the system remains robust even if the ICP and its RAM, ROM, and EEPROM are compromised. This is an extremely important feature of the present design, since these components of a chip are particularly vulnerable to both invasive and non-invasive attacks. The CryptoFirewall controls the addition of rights keys to the protected memory and thereby prevents information obtained from one CRU from providing attackers with the ability to add rights keys to other CRUs without breaking the cryptography or performing an invasive attack. Even if rights keys are compromised, attackers cannot insert them behind the CryptoFirewall.

As can be seen, this text does not even remotely reference an algorithm. Further, such text merely addresses the ability to add keys to the cryptofirewall. Such keys are not a fixed algorithm as claimed.

In view of the above, Appellants respectfully request reversal of the rejections.

3. Claim 3 is Not Separately Argued

4. Claim 4

Claim 4 provides that the custom logic block is implemented in solid state hardware that

implements a simple and well defined state machine. In rejecting these claims, the Office Action relies on Kocher col. 4, lines 1 to 13 which provide as follows:

> Commercially-deployed approaches usually use tamper-resistant hardware modules to enforce the content provider's access policies. FIG. 1 shows a smartcard of the background art for regulating access to encrypted content. The exemplary system includes three types of memory 110: ROM 115, EEPROM 125, and RAM 120. Each type of memory has advantages and disadvantages. ROM is fast and inexpensive, but cannot be modified and can often be read using advanced imaging techniques. RAM is fast and can be updated quickly, but loses its contents when power is lost. EEPROM retains its contents even when power is disconnected, but is relatively expensive to manufacture and is quite slow to modify.

Such text does not even mention a state machine or solid state hardware. Further, an electronic search of Kocher for the term "solid" provides no results. Without even mentioning solid state hardware or state machine, Kocher cannot possibly teach this claim.

In view of the above, Appellants respectfully request reversal of the rejections.

5. Claim 5 Is Not Separately Argued

6. Claim 6 Is Not Separately Argued

7. Claim 7 Are Not Separately Argued

B. Whether claims 8-28 are unpatentable under 35 U.S.C. §102(e) as being anticipated by Kocher, U.S. Patent 6,289,455 (Kocher).

1. Claims 8, 15, and 22

Appellants direct the attention of the Board to the arguments set forth above with respect to claim 1.

Further, Appellants respectfully traverse the rejection under 35 U.S.C. § 102(e) because the disclosure of Kocher fails to meet the threshold for anticipation, i.e. placing the public in possession of the claimed invention. Specifically, anticipation under 35 U.S.C. § 102 has strict requirements that all elements of the claim must be found in a single reference in order to support an anticipation rejection (see e.g. M.P.E.P. 2131). A claim is anticipated only when a single prior art reference discloses each and every limitation in the claim. See, e.g., *Glaxo Inc. v. Novopharm Ltd.,* 34 USPQ2d

1565 (Fed. Cir. 1995). The disclosure need not be express, but may anticipate by inherency where it would be appreciated by one of ordinary skill in the art. *Id.* See also *In re Robinson*, 49 USPQ2d 1949, 1950-51, (Fed. Cir. 1999) ("if the prior art reference does not expressly set forth a particular element of the claim, that reference still may anticipate if that element is 'inherent' in its disclosure. To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be recognized by persons of ordinary skill"). The requirement that an inherent element in a disclosure must be recognized by persons of ordinary skill in the art reflects the necessity that to constitute prior art under section 102, a reference must put subject matter into the possession of the public. See, e.g., *University of California v. Eli Lilly and Co.,* 43 USPQ2d 1398 (Fed. Cir. 1997). Therefore, in situations where an inherent element would not be recognized by persons of ordinary skill in the art, the reference cannot be anticipatory because a artisan cannot take the description of the invention in the printed publication, combine it with his own knowledge of the particular art, and from this combination be put in possession of the invention on which a patent is sought. See, e.g., *In re LeGrice*, 133 USPQ 365 (C.C.P.A. 1965).

In view of the above, Appellants submit that the use of a charge pump as claimed is not an inherent element of Kocher and would not be recognized by persons of ordinary skill in the art. In this regard, Kocher cannot be anticipatory nor can it be used to reject the claims under 35 U.S.C. §102.

Further, under MPEP §2142 and 2143.03 "To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970)." In this regard, the claim limitations regarding the sharing of programming charge pumps and programming control cannot merely be ignored or bypassed when rejecting the claims. Nor can such language merely be bypassed by stating that the claims merely recite the use of a charge pump without acknowledging or even addressing the sharing of the charge pumps among multiple nonvolatile memories or the manner and context in which the charge pump is being used.

In addition, the claims provide that the physical and logical address ranges are the same in

both the protected and non-protected nonvolatile memory components. Such a limitation is clearly not anticipated by Kocher under 35 U.S.C. §102(e).

In view of the above, Appellants respectfully request reversal of the rejections.

2. Claims 9, 16, and 23

These claims provide that the custom logic block has a fixed algorithm that cannot be altered by external means. In rejecting this claim, the Office Action relies on Kocher col. 23, lines 36 to 48. These lines provide:

> Under the architecture outlined in FIG. 2, the system remains robust even if the ICP and its RAM, ROM, and EEPROM are compromised. This is an extremely important feature of the present design, since these components of a chip are particularly vulnerable to both invasive and non-invasive attacks. The CryptoFirewall controls the addition of rights keys to the protected memory and thereby prevents information obtained from one CRU from providing attackers with the ability to add rights keys to other CRUs without breaking the cryptography or performing an invasive attack. Even if rights keys are compromised, attackers cannot insert them behind the CryptoFirewall.

As can be seen, this text does not even remotely reference an algorithm. Further, such text merely addresses the ability to add keys to the cryptofirewall. Such keys are not a fixed algorithm as claimed.

In view of the above, Appellants respectfully request reversal of the rejections.

3. Claims 10, 17, and 24 Are Not Separately Argued

4. Claims 11, 18, and 25

Claims 11, 18, and 25 provide that the custom logic block is implemented in solid state hardware that implements a simple and well defined state machine. In rejecting these claims, the Office Action relies on Kocher col. 4, lines 1 to 13 which provide as follows:

> Commercially-deployed approaches usually use tamper-resistant hardware modules to enforce the content provider's access policies. FIG. 1 shows a smartcard of the background art for regulating access to encrypted content. The exemplary system includes three types of memory 110: ROM 115, EEPROM 125, and RAM 120. Each type of memory has advantages and disadvantages. ROM is fast and inexpensive, but cannot be modified and can often be read using advanced imaging techniques. RAM is fast and can be updated quickly, but loses its contents when power is lost. EEPROM retains its contents even when power is disconnected, but is relatively expensive to manufacture and is quite slow to modify.

Such text does not even mention a state machine or solid state hardware. Further, an electronic search of Kocher for the term "solid" provides no results. Without even mentioning solid state hardware or state machine, Kocher cannot possibly teach this claim.

In view of the above, Appellants respectfully request reversal of the rejections.

5. Claims 12, 19, and 26 Are Not Separately Argued

6. Claims 13, 20, and 27 Are Not Separately Argued

7. Claims 14, 21, and 28 Are Not Separately Argued

C. Whether claims 1, 8, 15, and 22 are patentable under the judicially created doctrine of obviousness type double patenting over claims 1, 10, 19, and 28 of application serial number 10/085,346.

Appellants note that the subject matter of the copending application and the present application may change thereby obviating the need for the submission of a terminal disclaimer. Appellants may be willing to submit a terminal disclaimer should one become necessary. Therefore, at this time, Appellants traverse the rejection while reserving the right to submit a terminal disclaimer at a later date and upon the determination of allowable subject matter.

D. Conclusion

In light of the above arguments, Appellants respectfully submit that the cited references do not anticipate nor render obvious the claimed invention. More specifically, Appellants' claims recite novel physical features which patentably distinguish over any and all references under 35 U.S.C. §§ 102 and 103. As a result, a decision by the Board of Patent Appeals and Interferences reversing the Examiner and directing allowance of the pending claims in the subject application is respectfully solicited.

Respectfully submitted,

GATES & COOPER LLP

Attorneys for Appellant(s)

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: October 1, 2007

By: /Jason S. Feldmar/
Name: Jason S. Feldmar
Reg. No.: 39,187

JSF/kmk

G&C 109.70-US-01

## CLAIMS APPENDIX

1. A system for controlling access to digital services comprising:

(a) a control center configured to coordinate and provide digital services;

(b) an uplink center configured to receive the digital services from the control center and transmit the digital services to a satellite;

(c) the satellite configured to:

(i) receive the digital services from the uplink center;

(ii) process the digital services; and

(iii) transmit the digital services to a subscriber receiver station;

(d) the subscriber receiver station configured to:

(i) receive the digital services from the satellite;

(ii) control access to the digital services through an integrated receiver/decoder (IRD);

(e) a conditional access module (CAM) communicatively coupled to the IRD, wherein the CAM comprises:

(i) a protected nonvolatile memory component, wherein:

(1) the protected nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services;

(2) programming control and a programming charge pump are shared by both the protected nonvolatile memory component and a microprocessor's non-protected nonvolatile memory component; and

(3) the microprocessor's non-protected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same; and

(ii) a fixed state custom logic block configured to control access to the nonvolatile memory component, wherein data and address lines of the protected nonvolatile memory component are routed only to the fixed state custom logic block.

2. The system of claim 1 wherein the custom logic block has a fixed algorithm that cannot be altered by external means.

3. The system of claim 1 wherein access to a block of the protected nonvolatile memory component is limited to one or more functions defined in the custom logic block.

4. The system of claim 1 wherein the custom logic block is implemented in solid state hardware that implements a simple and well defined state machine.

5. The system of claim 1 wherein the protected nonvolatile memory component is not accessible through a system input/output module, system bus, microprocessor, or external environment.

6. The system of claim 1 wherein the nonvolatile memory component is exclusively controlled through the custom logic block and does not require the use of a system bus or microprocessor.

7. The system of claim 1 wherein a microprocessor's nonvolatile memory component and the protected nonvolatile memory component use the same physical and logical address ranges.

8. A method for limiting unauthorized access to digital services comprising:

(a) configuring a protected nonvolatile memory component, wherein:

(i) the protected nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services;

(ii) programming control and a programming charge pump are shared by both the protected nonvolatile memory component and a microprocessor's non-protected nonvolatile memory component; and

(iii) the microprocessor's non-protected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same;

(b) controlling access to the nonvolatile memory component through a fixed state custom logic block, and wherein data and address lines of the protected nonvolatile memory component are routed only to the fixed state custom logic block.

9. The method of claim 8 wherein the custom logic block has a fixed algorithm that cannot be altered by external means.

10. The method of claim 8 wherein access to a block of the protected nonvolatile memory component is limited to one or more functions defined in the custom logic block.

11. The method of claim 8 wherein the custom logic block is implemented in solid state hardware that implements a simple and well defined state machine.

12. The method of claim 8 wherein the protected nonvolatile memory component is not accessible through a system input/output module, system bus, microprocessor, or external environment.

13. The method of claim 8 wherein the nonvolatile memory component is exclusively controlled through the custom logic block and does not require the use of a system bus or microprocessor.

14. The method of claim 8 wherein a microprocessor's nonvolatile memory component and the protected nonvolatile memory component use the same physical and logical address ranges.

15. A conditional access module (CAM), comprising:

(a) a protected nonvolatile memory component, wherein:

(i) the protected nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing digital services;

(ii) programming control and a programming charge pump are shared by both the protected nonvolatile memory component and a microprocessor's non-protected nonvolatile memory component; and

(iii) the microprocessor's non-protected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same; and

(b) a fixed state custom logic block configured to control access to the nonvolatile memory component, and wherein data and address lines of the protected nonvolatile memory component are routed only to the fixed state custom logic block.

16. The CAM of claim 15 wherein the custom logic block has a fixed algorithm that cannot be altered by external means.

17. The CAM of claim 15 wherein access to a block of the protected nonvolatile memory component is limited to one or more functions defined in the custom logic block.

18. The CAM of claim 15 wherein the custom logic block is implemented in solid state hardware that implements a simple and well defined state machine.

19. The CAM of claim 15 wherein the protected nonvolatile memory component is not accessible through a system input/output module, system bus, microprocessor, or external environment.

20. The CAM of claim 15 wherein the nonvolatile memory component is exclusively controlled through the custom logic block and does not require the use of a system bus or microprocessor.

21. The CAM of claim 15 wherein a microprocessor's nonvolatile memory component and the protected nonvolatile memory component use the same physical and logical address ranges.

22. An article of manufacture for preventing unauthorized access to digital services comprising:

(a) means for configuring a protected nonvolatile memory component, wherein:

(i) the protected nonvolatile memory component is used to contain state information to provide desired functionality and enforce one or more security policies for accessing the digital services;

(ii) programming control and a programming charge pump are shared by both the protected nonvolatile memory component and a microprocessor's non-protected nonvolatile memory component; and

(iii) the microprocessor's non-protected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same; and

(b) means for controlling access to the nonvolatile memory component through a fixed state custom logic block, and wherein data and address lines of the protected nonvolatile memory component are routed only to the fixed state custom logic block.

23. The article of manufacture of claim 22 wherein the custom logic block has a fixed algorithm that cannot be altered by external means.

24. The article of manufacture of claim 22 wherein access to a block of the protected nonvolatile memory component is limited to one or more functions defined in the custom logic block.

25. The article of manufacture of claim 22 wherein the custom logic block is implemented in solid state hardware that implements a simple and well defined state machine.

26. The article of manufacture of claim 22 wherein the protected nonvolatile memory component is not accessible through a system input/output module, system bus, microprocessor, or external environment.

27. The article of manufacture of claim 22 wherein the nonvolatile memory component is exclusively controlled through the custom logic block and does not require the use of a system bus or microprocessor.

28. The article of manufacture of claim 22 wherein a microprocessor's nonvolatile memory component and the protected nonvolatile memory component use the same physical and logical address ranges.

## EVIDENCE APPENDIX

None.

## RELATED PROCEEDINGS APPENDIX

None.